УДК 004.7 DOI 10.37468/2307-1400-2024-2-25-41

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ DoS АТАК В VoIP-СИСТЕМАХ

Макарова Александра Константиновна [1]
Гельфанд Артем Максимович [1]
Поляничева Анна Валерьевна [1]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия

АННОТАЦИЯ

Статья посвящена проблеме обнаружения DoS атак на VoIP-систему. В интересах этого проводится ретроспективный анализ соответствующих методов, а именно, следующих пяти: ручное администрирование, экспертные правила, статистические правила, применение сигнатур и технологии искусственного интеллекта. Описываются идеи методов, приводятся их блок-схемы, даются примеры работы, оценивается их общая эффективность. Для сравнения методов выделяются следующие критерии: точность обнаружения, точность срабатывания, время подготовки, время срабатывания, человеческая ресурсоэкономность, программно-аппаратная ресурсоэкономность, интеллектуальность, простота реализации. Исходя из критериального сравнения сделаны основополагающие выводы касательно методов и их развития. Делаются выводы касательно путей продолжения исследования.

Ключевые слова: VoIP-система, DoS атаки, обнаружение, методы, ретроспективный анализ, критериальное сравнение.

RETROSPECTIVE ANALYSIS OF METHODS FOR DETECTING DoS ATTACKS IN VoIP SYSTEMS

Makarova Aleksandra K. [1]
Gelfand Artem M. [1]
Polyanicheva Anna V. [1]

[1] The Bonch-Bruevich Saint-Petersburg state university of telecommunications, Saint-Petersburg, Russia

ABSTRACT

The article is devoted to the problem of detecting DoS attacks on a VoIP system. To this end, a retrospective analysis of the relevant methods is carried out, namely the following five, namely the following five: manual administration, expert rules, statistical rules, the use of signatures and artificial intelligence technologies. The ideas of the methods are described, their flowcharts are given, examples of work are given, and their overall effectiveness is assessed. To compare methods, the following criteria are highlighted: detection accuracy, response accuracy, preparation time, response time, human resource efficiency, hardware and software resource efficiency, intelligence, ease of implementation. Based on the criterion comparison, fundamental conclusions were drawn regarding the methods and their development. Conclusions are drawn regarding ways to continue the research.

Keywords: VoIP system, DoS attacks, detection, methods, retrospective analysis, criterion comparison.

Введение

Повышение уровня коммуникации людей стало одним из основных трендов современного IT-мира. Так, VoIP-телефония позволила объединить людей в любых точках мира с использованием большого количества разнообразных устройств, и при этом, не ограничиваясь обычной голосовой связью. Тем не менее, с применением данной технологии существует и ряд проблем, одной из которых является ее подверженность ее информационным атакам. Так, проведение DoS атак на VoIP-системы может привести не только к нарушению качества связи между абонентами, но и попросту нарушить функционирование всей системы [1, 2]. Для того чтобы понять, как наиболее эффективно противодействовать такого рода атакам, одним из подходов может быть так называемый *ретроспективный анализ*, суть которого заключается в изучении исторических сведений – т.е. полученных из прошлого. Далее в работе будут рассмотрены основные методы обнаружения DoS атак, применимые к VoIP-системам, в порядке их исторической эволюции; за этим последует сравнение методов по ряду критериев.

Хронология методов

Приведем основные методы обнаружения DoS атак, применимые к VoIP-системам.

Метод 1. Ручное администрирование

Изначально методы защиты были в большей степени завязаны на людях, от которых в свою очередь и зависела безопасность всей системы [3]. Все лежало на плечах человека, который не только настраивал нормальное функционирование системы, корректировал, но и защищал ее. В данном методе не применяется как такового алгоритма и все ложится на плечи человека – администратора.

Администратор самостоятельно поддерживает систему в работоспособном состоянии и обеспечивает ее защиту. Он своими силами настраивает систему, просматривает и анализирует сетевой трафик на наличие аномальной активности и в случае сбоев или неработоспособности какого-либо сервиса начинает с помощью своих профессиональных навыков решать проблему. Если идет большая нагрузка на сеть, администратор также самостоятельно принимает решение о наличии угрозы. Например, если администратору сообщают о неработоспособности какого-либо сервиса, он проверяет данную информацию и предпринимает действия по устранению проблемы. Эффективность данного метода в большей степени зависит только от опыта человека и его профессионального мастерства.

Пример блок-схемы метода, отражающий его основную логику, представлен на рисунке 1.

Приведем описание основных элементов блок-схемы метода (см. рисунок 1).

Элемент «Начало» соответствует началу деятельности администратора.

Элемент «Цикл k от 1 до 144 (выполняется 1 день)» означает, что тело цикла будет выполняться 144 раза (фактически, 1 день).

Элемент «Администратор обновляет политики безопасности компании» соответствует действию администратора, связанному с обновлением политик компании.

Элемент «Найдено нарушение политики безопасности?» соответствует проверке события в части детектирования DoS атак.

Элемент «Цикл j от 1 до 10 (выполняется 10 минут)» означает, что тело цикла будет выполняться 10 раз (фактически, 10 минут).

Элемент «Администратор проверяет почту» соответствует действию администратора, связанному с проверкой корпоративной почты.

Элемент «Получено сообщение об инциденте?» соответствует проверке почты на предмет информирования о найденной неисправности или отключении сервиса, в части детектирования DoS атак.

Элемент «Цикл I от 1 до 60 (выполняется 1 минуту)» означает, что тело цикла будет выполняться 60 раз.

Элемент «Администратор проверяет сетевой трафик» соответствует действию администратора, связанному с анализом и мониторингом сетевого трафика в корпоративной сети.

Элемент «Объем трафика аномально увеличился?» соответствует проверке есть ли аномалии в трафике, в части детектирования DoS атак.

Элемент «Ждать 1 секунду» ? прерывание процесса мониторинга трафика.

Элемент «i увеличивается на 1» соответствует концу цикла, в котором администратор просматривает сетевой трафик каждую секунду.

Элемент «j увеличивается на 1» соответствует концу цикла, в котором администратор проверяет почту.

Элемент «k увеличивается на 1» соответствует концу цикла, в котором администратор обновляет политики безопасности.

Элемент «Вывод о начале DoS атаки» соответствует решению администратора об угрозе DoS атаки.

Элемент «Конец» соответствует концу деятельности администратора.

Приведем гипотетический пример работы метода. Администратор проверяет корпоративную почту, на которую сотрудники компании присылают ему вопросы и заявки на помощь. От сотрудницы А приходит письмо с просьбой разобраться в неработоспособности какого-либо сервиса.

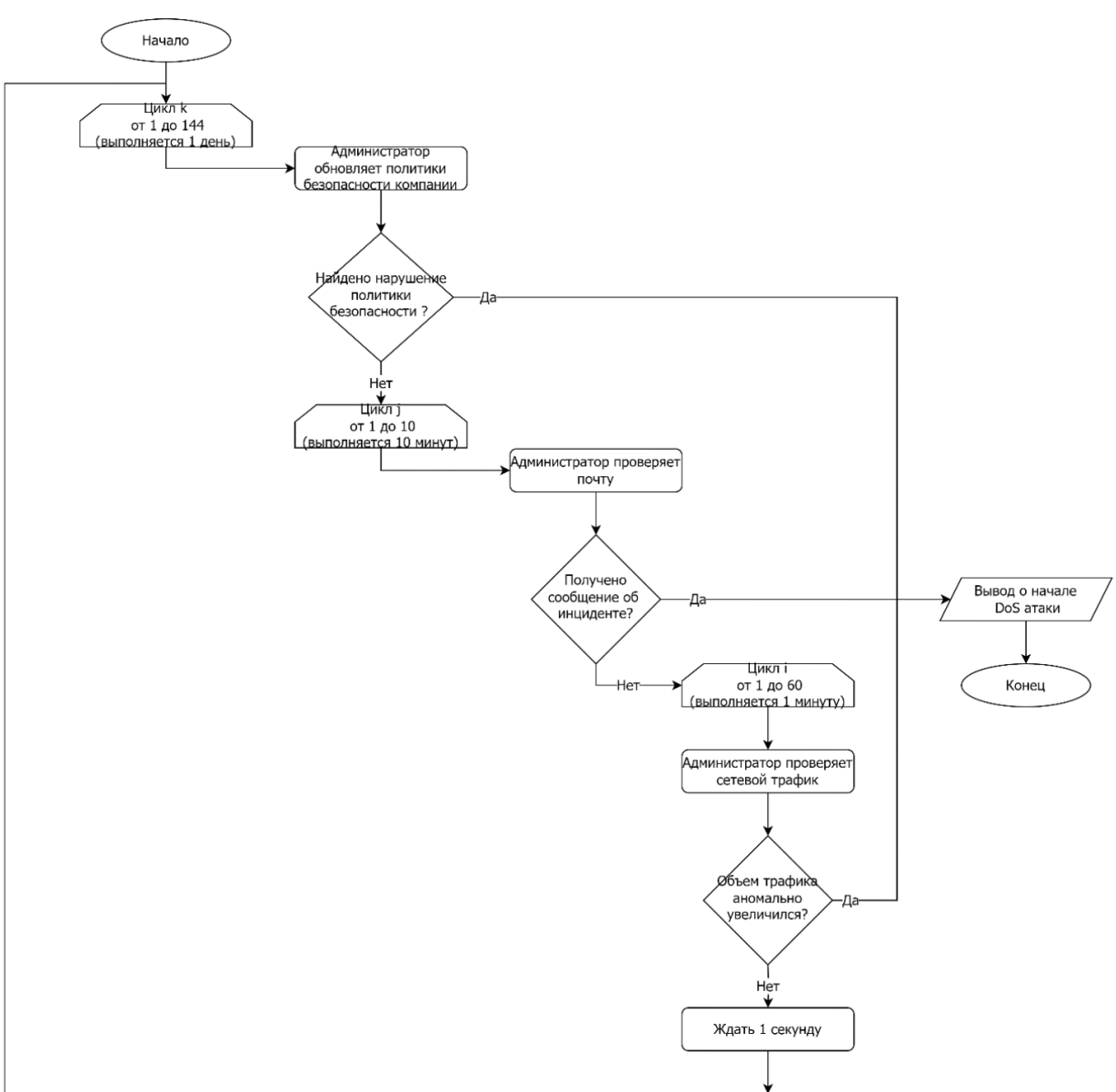

Рисунок 1 – Блок-схема метода обнаружения SIP-атак на основе ручного администрирования

Если неработоспособность сервиса (согласно профессиональному опыту и знанию администратора) связана с перегрузкой сети, которая в свою очередь связана с реализуемой в данный момент времени DoS атакой, то администратор принимает решение о начале контрмер по противодействию ей.

С точки зрения эффективности ее показатели для данного метода можно оценить следующим образом:

1) результативность – низкая, поскольку полностью опирается на опыт данного администратора, подверженного отрицательному влиянию человеческого фактора (усталость, злонамеренность, безответственность и т.д.);

2) оперативность – низкая, поскольку завязана на деятельности человека не использующего средства автоматизации;

3) ресурсоэкономность – средне низкая, поскольку идет существенная трата человеческого ресурса, но при этом затраты на программно-аппаратные ресурсы незначительные.

Метод 2. Экспертные правила

В данном методе производится частичная автоматизация с целью нейтрализации влияния человеческого фактора [4]. В Методе 1 все лежало на плечах человека, который полностью обеспечивал сопровождение системы; в отличие от него, в данном методе используется алгоритм, автоматизирующий работу администратора, который осуществляет лишь его настройку. В данном методе все еще есть влияние человеческого фактора, но оно не так велико, если не учитывать, что работу по предотвращению атаки возьмет на себя человек (администратор).

Идея метода заключается в следующем. По заданным администратором параметрам, программная реализация метода сама определяет начало DoS атаки. Администратор задает промежуток времени (T), равный размеру массива собираемых данных и предельно допустимое значение (L), равное максимальному допустимому количеству передаваемых в данный промежуток времени пакетов. Предельное значение (L) – это некий лимит, который нельзя превышать и активность выше которого считается атакой. Так, в данном методе человек только настраивает систему, а система в свою очередь уже следит за трафиком, считает его и в случае превышения сигнализирует о начавшейся DoS атаке. Предельное значение (L) меняется в зависимости от обстоятельств, поэтому человек вряд ли всегда сможет учитывать все факторы, влияющие на кол-во пакетов, передаваемых по сети.

Пример блок-схемы метода, отражающий его основную логику, представлен на рисунке 2.

Приведем описание основных элементов блок-схемы метода (см. рисунок 2).

Элемент «Начало» соответствует началу работы программы.

Элемент «Ввод размера окна трафика в секундах (T)» означает, что администратор вводит промежуток времени, за который будет считаться сумма пакетов для проверки на превышение предела.

Элемент «Ввод предельно допустимого количества пакетов (L)» означает, что администратор вводит предельно допустимое значение количества пакетов.

Элемент «Инициализация S = 0» означает, что создается переменная S, в которой будет считаться сумма пакетов.

Элемент «Создание очереди FIFO размера T (O)» означает, что начинается подсчет пакетов и создается очередь элементов.

Элемент «Подсчет кол-ва пакетов за секунду (n)» означает, что программа считает, какое количество пакетов прошло по сети в данную секунду.

Элемент «S = S + n - O [1]» означает, что происходит подсчет суммы и запись суммы в переменную S. Складывается имеющееся значение суммы (S) и последнее подсчитанное количество пакетов (n), при этом вычитая самое первое значение количества пакетов в списке (O [1]).

Элемент «Помещение n в начало очереди O» означает, что новое пришедшее число пакетов становится в конец очереди.

Элемент «Удаление значения в конце очереди O» означает, что значение в начале очереди O [1] удаляется из очереди.

Элемент «S > L?» означает сравнение текущей суммы пакетов (S) с предельно допустимым значением пакетов (L).

Элемент «Вывод о начале DoS атаки» означает, что программа сигнализирует администратору о превышении трафика и возможной угрозе DoS атаки.

Элемент «Конец» соответствует окончанию работы программы.

Приведем гипотетический пример работы метода. Администратор задает промежуток времени (T) и предельно допустимое значение количества пакетов (L) для сигнализации об атаке. Метод на основе введенных данных начинает считать пакеты и формирует очередь из значений количества пакетов за каждую секунду. Каждую секунду считается проходящее по сети количество пакетов и заносится в конец очереди, а первый элемент в очереди отбрасывается. Также каждую секунду считается суммарное прошедшее количество пакетов (S) в очереди за период времени (T). Значение переменной S сравнивается с предельно

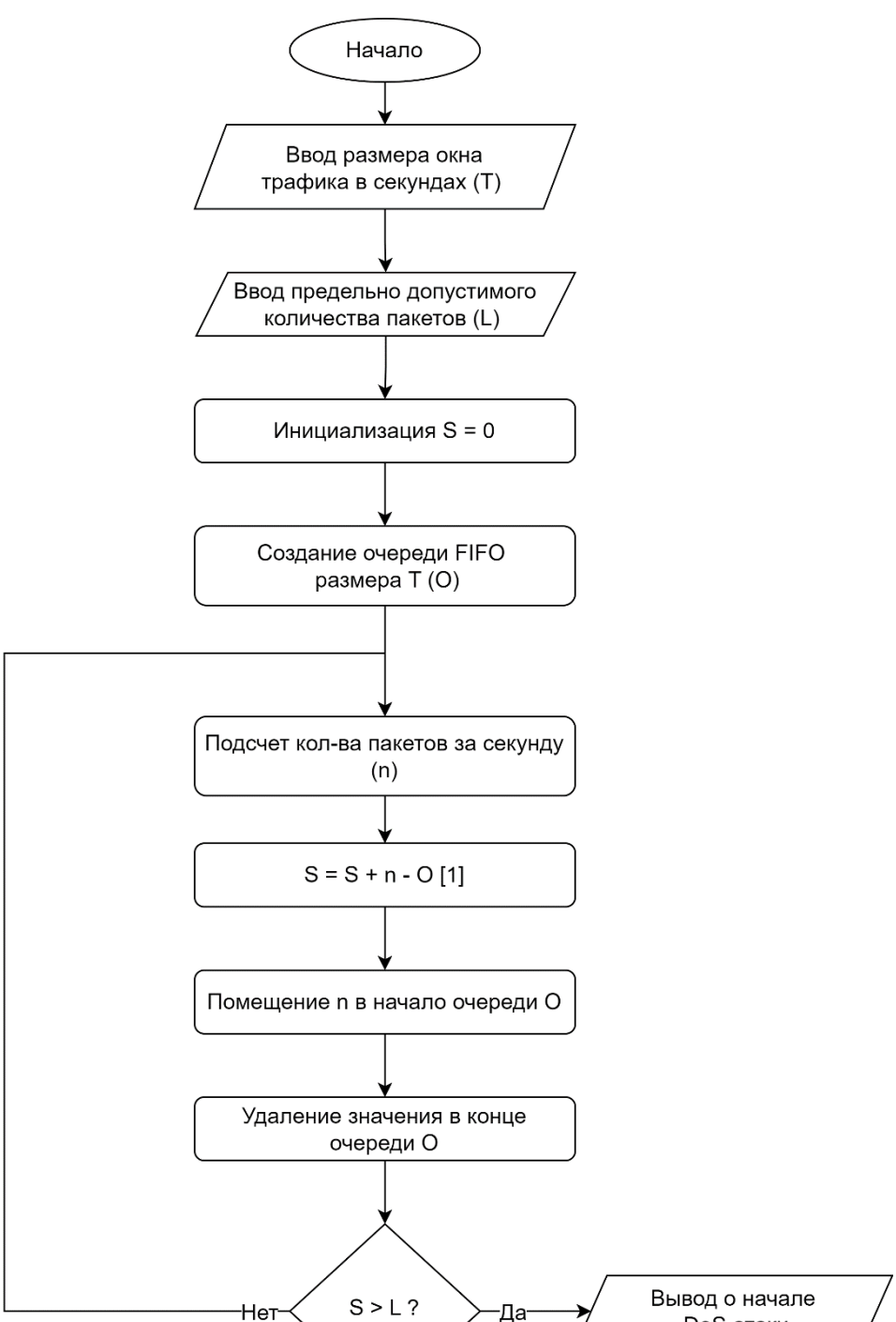

Рисунок 2 – Блок-схема метода обнаружения SIP-атак на основе экспертных правил

допустимым значением количества пакетов (L). В случае если значение S больше L, система информирует Администратора о начавшейся DoS атаке.

С позиции эффективности, метод может быть оценен следующим образом:

1) результативность – ниже среднего, поскольку автоматизация все еще опирается на представлении человека о максимально допустимом количестве пакетов. Человек сам вычисляет и выбирает это значение и может ошибочно его

ввести. При этом сам алгоритм достаточно тривиален и не всегда способен отличить высокую активность в сети от целенаправленной атаки.

2) оперативность – высокая, поскольку постоянно считает допустимое значение пакетов. В алгоритме отсутствуют подготовительные (предварительный сбор и анализ данных, обучение) и дополнительные (анализ полей пакетов, глубокий анализ трафика);

3) ресурсоэкономность – выше среднего, алгоритм не требует больших программно-аппаратных мощностей и не завязана на человеческом факторе, от администратора требуется ввод параметров только в начале работы.

Метод 3. Статистические правила

В данном методе увеличилась автоматизация процесса анализа трафика, поскольку часть параметров работы алгоритма устанавливаются на основании статистики [5]. Тем не менее, часть параметров администратор все также вынужден указывать алгоритму.

Идея метода заключается в следующем. После запуска программы алгоритм в течение времени (V), заданного администратором, следит за количеством пакетов (при нормальной работе системы VoIP) и определяет среднее количество пакетов за этот период (L). Таким образом, L – это лимит, который нельзя превышать и активность выше которого считается атакой. Затем работает тот же алгоритм, что и во втором методе, но накапливая новое среднее значение (т.е. обновляя L). Так, алгоритм накапливает значение L на каждый следующий месяц работы.

В данном методе человек только вводит начальные параметры, а система собирает статистику и по ней следит за трафиком. Предельное значение (L) меняется в зависимости от «ситуации» (например, времени года или отпусков сотрудников), поэтому в методе влияние человеческого фактора снижено.

Пример блок-схемы метода, отражающий его основную логику, представлен на рисунке 3.

Приведем описание основных элементов блок-схемы метода (см. рисунок 3).

Элемент «Начало» соответствует началу работы программы.

Элемент «Ввод размера окна трафика в сек. (T)» означает, что администратор вводит промежуток времени, за который будет считаться сумма пакетов для проверки на превышение предела.

Элемент «Ввод времени сбора статистики в сек. (V)» означает, что администратор вводит промежуток времени, за который будет осуществлять сбор статистики для получения среднего допустимого значения (L).

Элемент «Ввод коэф. превышения среднего (K)» означает, что администратор вводит коэффициент капризности системы, который отвечает за чувствительность реагирования на превышение количества пакетов.

Элемент «Количество пакетов за время V: W = 0» означает, что программа инициализирует переменную W, отвечающую за общее количество пакетов за время V.

Элемент «Цикл i от 1 до V в секундах» означает, что тело цикла будет выполняться V раз (сбор статистики – месяц).

Элемент «Подсчет количества пакетов за 1 секунду (n)» означает, что программа считает пакеты, пришедшие за каждую секунду.

Элемент «W = W + n» означает, что в переменную W прибавляется количество пакетов за каждую секунду. Программа считает сумму всех пришедших пакетов.

Элемент «i увеличивается на 1» соответствует концу цикла, в котором происходит подсчет общего количества пакетов за период времени V.

Элемент «Среднее количество пакетов в окне: L = W / V * T» означает, что в переменной L подсчитывается среднее количество пакетов, пришедших за время V, в размере окна трафика T. Программа считает предельно допустимое количество пакетов L.

Элемент «Инициализация S = 0» означает, что создается переменная S, в которой будет считаться сумма пакетов за промежуток времени T.

Элемент «Создание очереди FIFO размера T (O)» означает, что начинается подсчет пакетов и создается очередь элементов.

Элемент «W = 0» соответствует обнулению

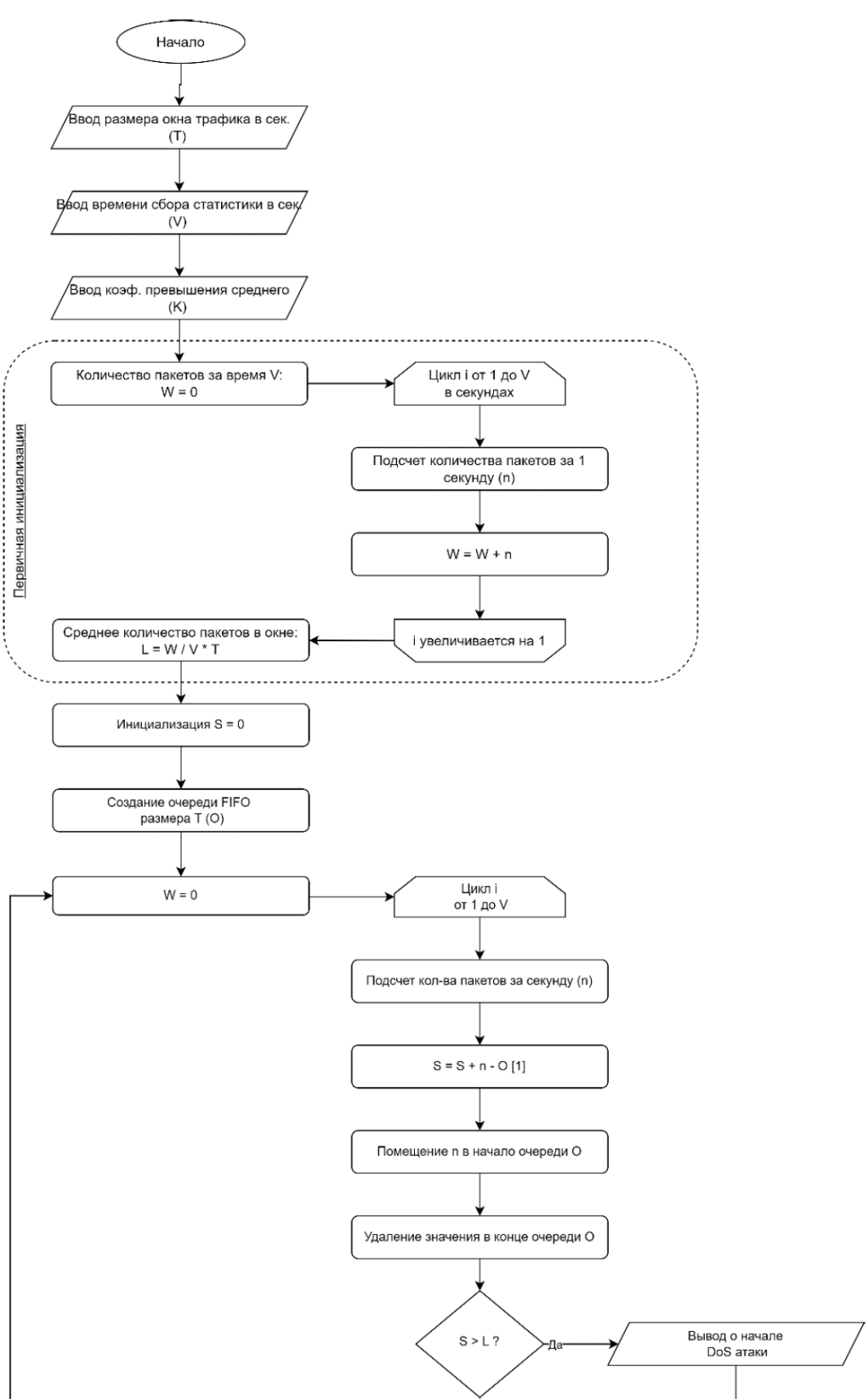

Рисунок 3 – Блок-схема метода обнаружения SIP-атак на основе статистических правил

переменной W для дальнейшего подсчета суммы всех пакетов, пришедших за время V.

Элемент «Цикл i от 1 до V» означает, что тело цикла будет выполнятся V раз.

Элемент «Подсчет кол-ва пакетов за секунду (n)» означает, что программа считает, какое количество пакетов прошло по сети в данную секунду.

Элемент «S = S + n - O [1]» означает, что происходит подсчет суммы и запись суммы в переменную S. Складывается имеющееся значение суммы (S) и последнее подсчитанное количество пакетов (n), при этом вычитая самое первое значение количества пакетов в списке (O [1]).

Элемент «Помещение n в начало очереди O» означает, что новое пришедшее число пакетов становится в конец очереди.

Элемент «Удаление значения в конце очереди O» означает, что значение в начале очереди O [1] удаляется из очереди.

Элемент «S > L?» означает сравнение текущей суммы пакетов (S) с предельно допустимым значением пакетов (L).

Элемент «W = W + n» означает, что в переменную W прибавляется количество пакетов за каждую секунду. Программа считает сумму всех пришедших пакетов.

Элемент «i увеличивается на 1» соответствует концу цикла. Считается сумма пакетов (S) за период времени (T) и сравнивается с пределом (L). Также обновляется значение в переменной W – общее количество пакетов за время V.

Элемент «L = W / V * T» означает, что в переменной L подсчитывается среднее количество пакетов, пришедших за время V, в размере окна трафика T. Программа считает предельно допустимое количество пакетов L.

Элемент «Вывод о начале DoS атаки» означает, что программа сигнализирует администратору о превышении трафика и возможной угрозе DoS атаки.

Элемент «Конец» соответствует окончанию работы программы.

Приведем гипотетический пример работы метода. Администратор в начале работы алгоритма задает 3 значения: промежуток времени (T) по аналогии с Методом 2, время сбора статистики (V, где V >> T) и коэффициент превышения (K). Метод за период введенного времени (V) начинает считать пакеты для получения среднего допустимого количества пакетов (L) для начала своей работы. Затем алгоритм начинает работать аналогично Методу 2 – в каждую секунду считается проходящее по сети количество пакетов и заносится в конец очереди, первый элемент в очереди отбрасывается. Также каждую секунду считается суммарное прошедшее количество пакетов (S) в очереди за период времени (T). Значение переменной S сравнивается с предельно допустимым значением количества пакетов (L). После месяца работы программы вычисляется новая L. В случае если значение S больше L, система информирует Администратора о начавшейся DoS атаке.

С позиции эффективности, метод может быть оценен следующим образом:

1) результативность – средняя, поскольку полная автоматизация происходит только со второго месяца работы алгоритма. При этом, данный метод продолжает опирается на опыт администратора, пробуя, вычислять оптимальное значение коэффициента K, чтобы минимизировать ложные срабатывания системы.

2) оперативность – выше среднего, поскольку прежде, чем объективно оценивать, программа в течение месяца должна собирать статистику. Несмотря на это, программа постоянно считает допустимое значение пакетов;

3) ресурсоэкономность – выше среднего, т.к. алгоритм все также не требует больших программно-аппаратных мощностей и не завязан на человеческом факторе. Администратору лишь требуется ввести параметры для сбора данных и коэффициент чувствительности в начале работы.

Метод 4. Сигнатурный

Данный метод на основе сигнатурного анализа является более точным предыдущих; также его алгоритм имеет более высокий уровень автоматизации [6]. В данном методе администратору необходимо выбрать два параметра определения близости атаки к заранее заданной сигнатуре, которая используется для принятия решения

о наличии атаки в системе VoIP. К особенностям метода можно отнести следующие: отсутствует период сбора статистики, а алгоритм начинает работать сразу после ввода параметров.

Суть метода заключается в построении экспоненциальной закономерности на основе собранных за промежуток времени (T) пакетов (n) в VoIP-системе. Также человеком (администратором) для работоспособности алгоритма один раз в начале его работы вводятся следующие параметры: коэффициент K – значение, определяющее минимальную «крутизну» экспоненты для детектирования сетевого трафика, как DoS атаки; коэффициент R – насколько можно доверять аппроксимации к экспоненте. Параметры K и R никак не зависят от трафика и выбираются администратором на основании политик компании и экспертного мнения. Пришедшие каждую секунду в промежуток времени (T) пакеты (n), образуют разброс точек относительно кривой, которая при резком возрастании (k) и высокой аппроксимации (r) воспринимается алгоритмом как начавшаяся DoS атака.

Пример блок-схемы метода, отражающий его основную логику, представлен на рисунке 4.

Приведем описание основных элементов блок-схемы метода (см. рисунок 4).

Элемент «Начало» соответствует началу работы программы.

Элемент «Ввод размера окна трафика в сек. (T)» означает, что администратор вводит промежуток времени, за который будет считаться сумма пакетов для проверки на превышение предела.

Элемент «Ввод коэффициента приближения (R)» означает, что администратор вводит значение R, которое отвечает за то, насколько близко количество пакетов n должно находиться к экспоненциальной кривой.

Элемент «Ввод коэффициента экспоненты (K)» означает, что администратор вводит значение K, которое отвечает за то, насколько «крутой» рост у полученной экспоненциальной кривой.

Элемент «Создание очереди FIFO размера T (O)» означает, что начинается подсчет пакетов и создается очередь элементов.

Элемент «Подсчет кол-ва пакетов за секунду (n)» означает, что программа считает, какое количество пакетов прошло по сети в данную секунду.

Элемент «Аппроксимация очереди O к кривой $y = e^{k(x+a)} + b$» означает, что программа строит такую экспоненциальную кривую, чтобы она была наиболее приближена ко всем точкам (количества пакетов n) за отрезок времени T.

Элемент «Получение параметров прямой a, k, b, r» означает, что программа подбирает параметры кривой по осям x, y и новые коэффициенты к ней.

Элемент «Помещение n в начало очереди O» означает, что новое пришедшее число пакетов становится в конец очереди.

Элемент «Удаление значения в конце очереди O» означает, что значение в начале очереди O [1] удаляются из очереди.

Элемент «r > R и k > K ?» Аппроксимация, вычисленная алгоритмом (r), не должна превышать значение введенной администратором и также значение коэффициента экспоненты (k), вычисленное алгоритмом, не должно быть выше введенного коэффициента экспоненты (K).

Элемент «Вывод о начале DoS атаки» означает, что программа на основании прошлого условия делает вывод об угрозе Dos атаки.

Элемент «Конец» соответствует окончанию работы программы.

Приведем гипотетический пример работы метода. Администратор задает 3 значения: промежуток времени (T) по аналогии с предыдущими методами, коэффициент минимального приближения к экспоненте (R) и коэффициент минимальной «крутости» роста экспоненты (K). Далее формируется очередь O размера T. На основе полученных значений количества пакетов (n) строится аппроксимация к кривой, после построения получаем параметры a, k, b, r, а каждую секунду считается проходящее по сети количество пакетов и заносится в конец очереди; первый элемент в очереди отбрасывается. Происходит сравнение аппроксимации, вычисленной алгоритмом (r) и введенного администратором значения, а также значение коэффициента экспо-

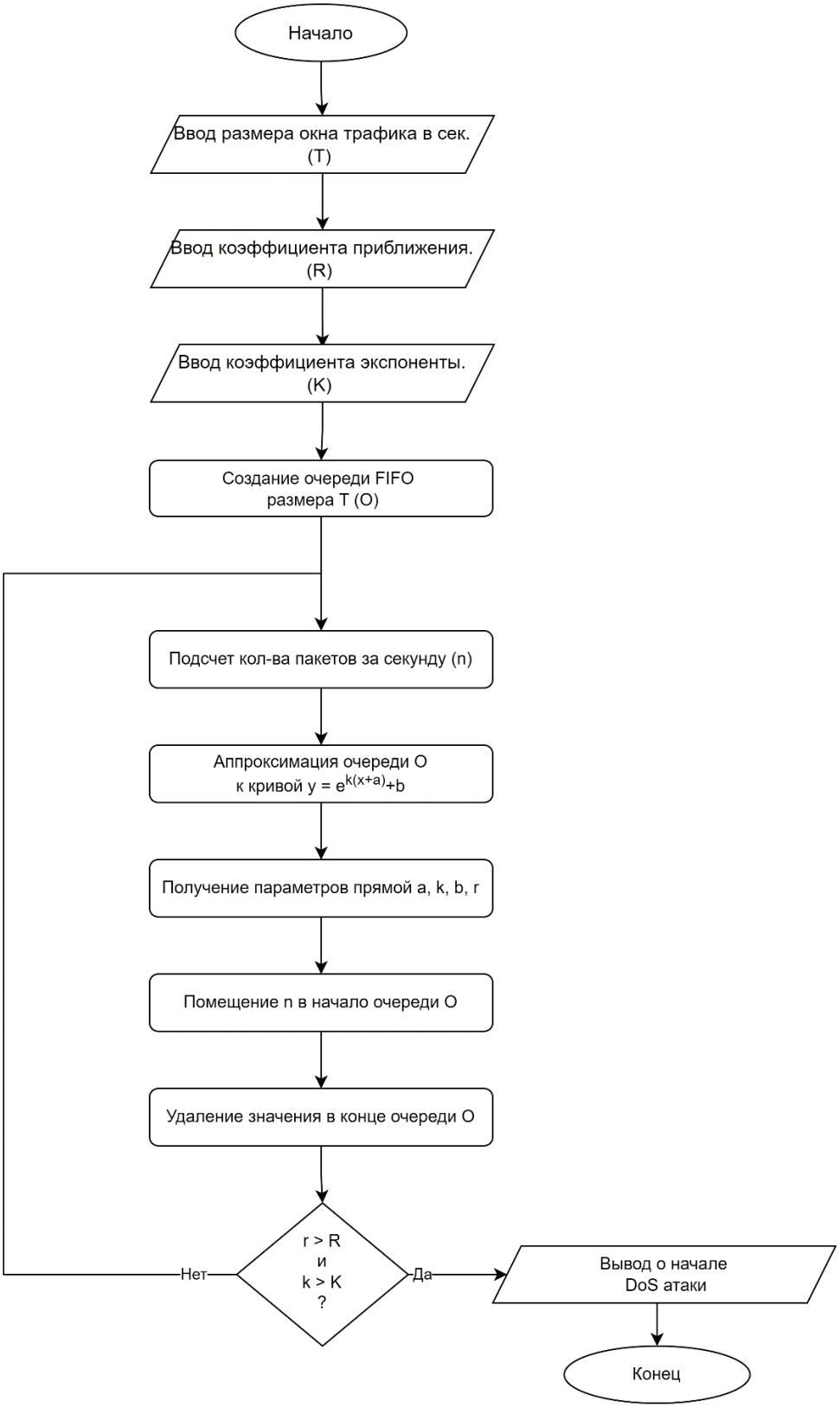

Рисунок 4 – Блок-схема метода обнаружения SIP-атак на основе сигнатур

ненты (k), вычисленное алгоритмом с введенным коэффициентом экспоненты (K). В случае если значения r и k превышают введенные, система информирует администратора о начавшейся DoS атаке.

С позиции эффективности, метод может быть оценен следующим образом:

1) Результативность – выше среднего, поскольку реализована полная автоматизация. Однако точность далека от идеала, поскольку для

определения атаки используется конкретная сигнатура, знание которой необходимо иметь человеку (администратору);

2) Оперативность – высокая, поскольку алгоритму не требуется период сбора статистики, и она сразу начинает делать выводы о возможной DoS атаке на систему;

3) Ресурсоэкономность – выше среднего, алгоритм все также не требует больших программно-аппаратных мощностей и не завязан на человеческий фактор.

Метод 5. Интеллектуальный

Алгоритм данного метода значительно автоматизирован за счет применения технологий искусственного интеллекта в части машинного обучения (МО) [8]. В ранее описанных методах окончательное решение о наличии атаки все еще опиралось на профессиональный опыт человека (администратора) из-за ввода соответствующих параметров (пределы, период сбора статистики и т.п.). В данном же методе система обнаружения вначале обучается на DoS атаках, а потом начинает их детектировать.

До ввода алгоритма в эксплуатацию производится обучение модели МО с помощью генерации разного типа трафика: обычного, имитирующего типовую работу пользователей и атакующего, созданного соответствующими генераторами атак. После обучения алгоритм переходит в режим стандартной работы.

Пример блок-схемы метода, отражающий его основную логику, представлен на рисунке 5.

Приведем описание основных элементов блок-схемы метода (см. рисунок 5).

Элемент «Начало» соответствует началу работы программы.

Элемент «Ввод размера окна трафика в сек. (T)» означает, что администратор вводит промежуток времени, за который будет считаться сумма пакетов для проверки на превышение предела.

Элемент «Генерация разного типа трафика (с атакой и без) длиной V» означает, что администратор задает время, за которое алгоритм будет обучаться на данных – трафик с атакой и без нее.

Элемент «Создание очереди FIFO размера T (O)» означает, что начинается подсчет пакетов и создается очередь элементов.

Элемент «Цикл i от 1 до V в секундах» означает, что тело цикла будет выполняться V раз (т.е. обучение модели МО).

Элемент «Подсчет кол-ва пакетов за секунду (n)» означает, что программа считает, какое количество пакетов прошло по сети в данную секунду.

Элемент «Помещение n в начало очереди O» означает, что новое пришедшее число пакетов становится в конец очереди.

Элемент «Удаление значения в конце очереди O» означает, что значение в начале очереди O [1] выкидывается из очереди.

Элемент «Обучение модели МО на очереди O» означает, что определенному шаблону очереди присваивается тип: либо атака, либо ее отсутствие.

Элемент «i увеличивается на 1» соответствует концу цикла, в котором обучается модель МО.

Элемент «Отчистка очереди O» означает, что алгоритм МО начинает работать с реальными данными трафика.

Элемент «Подсчет кол-ва пакетов за секунду (n)» означает, что программа считает, какое количество пакетов прошло по сети в данную секунду.

Элемент «Помещение n в начало очереди O» означает, что новое пришедшее число пакетов становится в конец очереди.

Элемент «Удаление значения в конце очереди O» означает, что значение в начале очереди O [1] выкидывается из очереди.

Элемент «Классификация очереди O по модели МО (C)» означает, что модель МО классифицирует полученную очередь (O) на основании своей базы данных классов.

Элемент «C = Атака?» означает, что алгоритм сравнивает, соответствует ли полученный класс атаке.

Элемент «Вывод о начале DoS атаки» означает, что программа на основании прошлого условия делает вывод об угрозе Dos атаки.

Элемент «Конец» соответствует окончанию работы программы

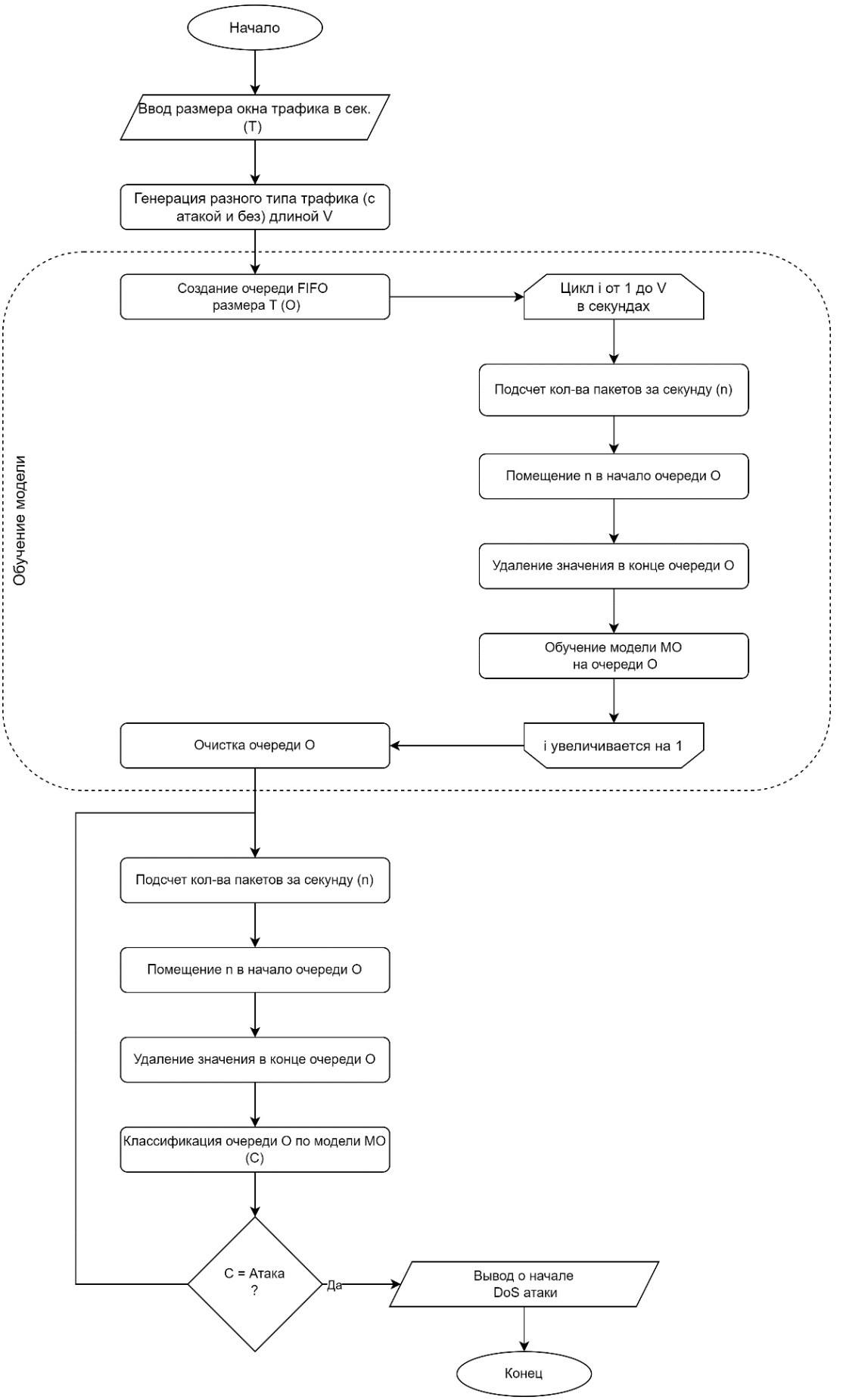

Рисунок 5 – Блок-схема метода обнаружения SIP-атак на основе машинного обучения

Приведем гипотетический пример работы метода.

Администратор задает 2 значения: промежуток времени (T) по аналогии с предыдущими методами и время (V), за которое модель будет обучаться на сгенерированном администратором трафике (обычном и содержащим атаки). Далее формируется очередь O размера T и каждый цикл модель обучается, классифицируя полученные очереди. Затем очередь отчищается для дальнейшего ввода алгоритма в условия реальной эксплуатации. После этого, уже в реальной сети, также каждую секунду формирует очереди, но уже классифицируемая на основе обученной модели МО. Если класс трафика соответствует атаке, то система информирует администратора об этом.

С позиции эффективности, метод может быть оценен следующим образом:

1) результативность – высокая, потому что может подстраиваться под самые сложные сценарии атак и является полностью автоматизированной;

2) оперативность – выше среднего, поскольку до начала работы алгоритму необходимо обучить модель МО на шаблонах и только спустя обучения приступить к работе. При том что сами шаблоны тоже необходимо сформировать;

3) ресурсоэкономность – выше среднего, алгоритм может требовать больших программно-аппаратных мощностей, но не завязан на человеческом факторе. Администратору требуется ввести один входной параметр – временной промежуток T.

Критериальный анализ

Произведем сравнение методов защиты от DoS атак на VoIP, с помощью проведения критериального анализа каждого из них. Были выделены следующие критерии (отражающие суть и отличительные особенности решений):

Точность обнаружения – насколько корректно данный метод может обнаружить реальную атаку;

Точность срабатывания – насколько метод не реагирует на обычное (т.е. легальное) повышение сетевой активности;

Скорость подготовки – насколько быстро данный метод готов к работе в условиях реально корпоративной сети;

Скорость срабатывания – насколько быстро метод может определять, что производится атака;

Человеческая ресурсоэкономность – ресурсоэкономность с точки зрения затраты человеческих ресурсов (количества специалистов, их уровня профессиональной подготовки);

Программно-аппаратная ресурсоэкономность – ресурсоэкономность с точки зрения затраты ресурсов на программное обеспечение и ее аппаратную поддержку;

Интеллектуальность – в какой степени применяется интеллектуальная составляющая [8];

Простота реализации – насколько низка трудоемкость для реализации метода.

Результаты сравнительного анализа разработанных методов по выделенным критериям приведены в таблице 1; приведем расшифровку их значений по шкале из 3-х значений (чем выше показатель сравнения, тем он лучше.): Н – это низко, С – это средне и В – это высокая.

Результаты сравнительного анализа (см. таблицу 1) позволяют сделать следующие выводы по каждому из критериев с учетом тенденции развития методов (т.е. от 1 до 5); сама гистограмма балльных значений критериев приведена на рисунке 6:

Таблица 1 – Критериальное сравнение методов обнаружения DoS атак

Методы	Критерии							
	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8
Метод 1. Ручное администрирование	Н	С	В	С	Н	В	Н	В
Метод 2. Экспертные правила	С	С	В	В	Н	С	Н	В
Метод 3. Статистические правила	С	С	Н	С	С	С	Н	С
Метод 4. Сигнатурный	В	В	В	В	В	С	С	Н
Метод 5. Интеллектуальный	В	В	С	С	В	Н	В	Н

– значение К_1 растет, поскольку методы эволюционируют по пути улучшения точности;

– значение К_2 также растет (более слабо, чем К_1), поскольку точность срабатывания также является важным фактором;

– значение К_3 у методов различно, что отражает специфику их алгоритмов, как использующих подготовительный эффект, так и включающийся в работу сразу;

– значение К_4 у всех методов достаточно высокое, что говорит об их общей высокой оперативности работы;

– значение К_5 в процессе эволюции методов растет, что говорит о постепенном отказе от ручного труда экспертов;

– в противовес К_5, значение К_6 методов уменьшается, поскольку отказ от человеческого участия ведет к нагрузке техники;

– значение К_7 растет, поскольку методы все чаще начинают применять инновационные достижения (в частности, искусственный интеллект);

– значение К_8 снижается, что говорит, что простые алгоритмы в принципе не способны «выдавать» высокую эффективность обнаружения DoS атак.

Таким образом (см. Рисунок 6), нельзя говорить о каком-либо наилучшем методе обнаружения атак (из рассмотренных), поскольку у каждого из них есть свои достоинства и недостатки.

Выводы

В работе произведен ретроспективный анализ методов обнаружения DoS атак, применимых для VoIP-систем. Как результат, выделены следующие 5 методов обнаружения, расположенных в процессе их эволюции: ручное администрирование, экспертные правила, статистические правила, применение сигнатур и технологии искусственного интеллекта. Произведено сравнение методов по следующим критериям: точность обнаружения, точность срабатывания, время подготовки, время срабатывания, человеческая ресурсоэкономность, программно-аппаратная ресурсоэкономность, интеллектуальность, простота реализации. Исходя из критериального сравнения сделаны основополагающие выводы касательно методов и их развития.

Продолжением исследования должна стать реализация методов, их оценка, развитие области применения [9], применение других подходов к обнаружению DoS атак (например, путем применения машинного обучения с подкреплением и нелинейных систем управления [10]), а также создание комплексного метода [11].

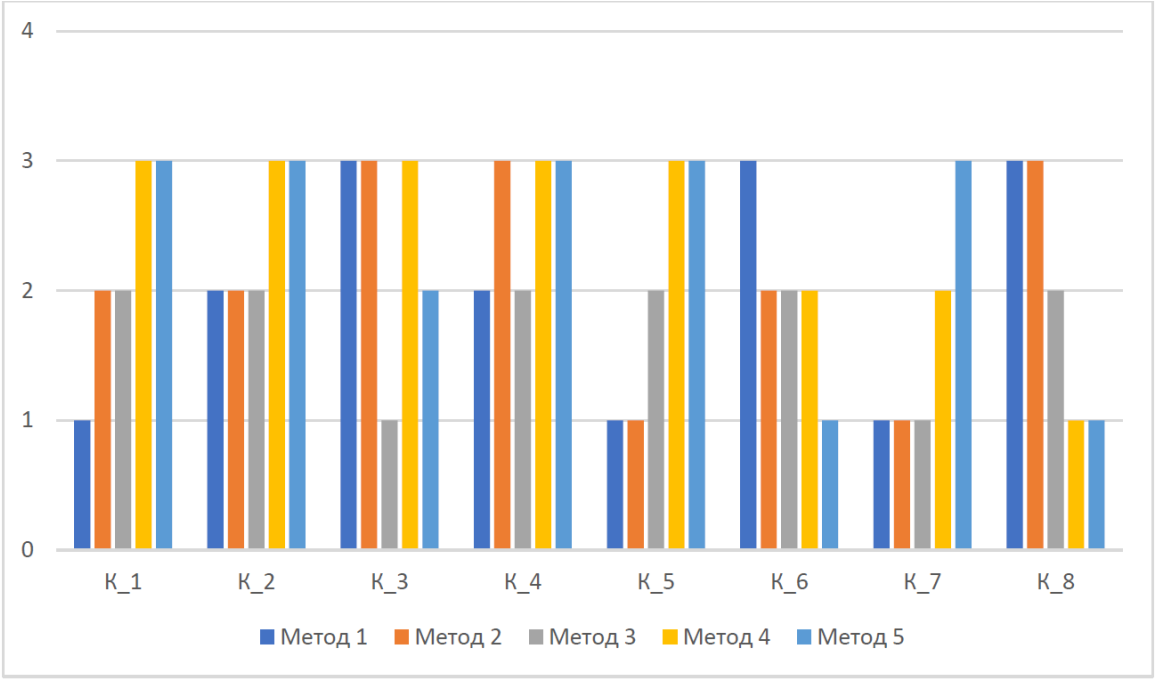

Рисунок 6 – Гистограмма балльных значений критериев для методов

Список литературы

1. *Израилов К.Е., Макарова А.К., Шестаков А.В.* Обобщенная модель защиты от кибератак на VOIP // Вопросы кибербезопасности. – 2023. – № 2(54). – С. 109-121. – DOI 10.21681/2311-3456-2023-2-109-121. – EDN KIMEAW.

2. *Макарова А.К., Поляничева А.В., Саматова К.А.* Анализ уязвимостей оборудования передачи голосового трафика // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022): сборник статей XI Международной научно-технической и научно-методической конференции (Санкт-Петербург, 15–16 февраля 2022 года). – Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2022. – С. 665-669. – EDN JRKJAR.

3. *Джиневэн Ш.* Администрирование в движении // Сети и системы связи. – 2007. – № 14. – С. 43-52. – EDN ILJELV.

4. *Хомоненко А.Д.* Согласование экспертных оценок при нечётком выводе в системе обнаружения вторжений // Проблемы информационной безопасности. Компьютерные системы. – 2009. – № 4. – С. 42-50. – EDN LDGKYP.

5. *Терновой О.С.* Раннее обнаружение DDoS атак на основе статистического анализа // Перспективы развития информационных технологий. – 2011. – № 6. – С. 212-215. – EDN RPDHNT.

6. *Борисов В.И., Шабуров А.С.* О применении сигнатурных методов анализа информации в SIEM-системах // Вестник УрФО. Безопасность в информационной сфере. – 2015. – № 3(17). – С. 23-27. – EDN VIYWEZ.

7. *Токарев С.А.* Исследование алгоритмов искусственного интеллекта для обнаружения сетевых атак // International Journal of Professional Science. – 2023. – № 6. – С. 177-182. – EDN TKYRXE.

8. *Орлов Г.А., Красов А.В., Гельфанд А.М.* Применение Big Data при анализе больших данных в компьютерных сетях // Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12, № 4. – С. 76-84. – DOI 10.36724/2409-5419-2020-12-4-76-84. – EDN RQQTOQ.

9. *Красов А.В., Гельфанд А.М., Коржик В.И.* Построение доверенной вычислительной среды [и др.]. – СПб: Индивидуальный предприниматель Петрив Роман Богданович, 2019. – 108 с. – ISBN 978-5-6043143-2-6. – EDN RECXBI.

10. *Душин С.Е., Красов А.В., Кузьмин Н.Н., Яковлев В.Б.* Синтез структурно-сложных нелинейных систем управления: Системы с полиномиальными нелинейностями. – СПб: Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), 2004. – 371 с.

11. *Браницкий А.А.* Комбинированный подход к обнаружению сетевых атак на основе сигнатурного анализа и методов вычислительного интеллекта // Региональная информатика «РИ-2016» : Материалы конференции, Санкт-Петербург, 26–28 октября 2016 года. – Санкт-Петербург: Политехника-принт, 2016. – С. 150. – EDN OTYTAX.

References

1. *Izrailov K.E., Makarova A.K., Shestakov A.V.* Generalized model of protection against cyberattacks on VOIP // Cybersecurity Issues. - 2023. - No. 2 (54). - P. 109-121. - DOI 10.21681 / 2311-3456-2023-2-109-121. - EDN KIMEAW.

2. *Makarova A.K., Polyanicheva A.V., Samatova K.A.* Analysis of vulnerabilities of voice traffic transmission equipment // Actual problems of infotelecommunications in science and education (APINO 2022): collection of articles of the XI International Scientific, Technical and Scientific-Methodological Conference (St. Petersburg, February 15-16, 2022). – Volume 1. – Saint Petersburg: Saint Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2022. – P. 665-669. – EDN JRKJAR.

3. *Dzhinevan Sh.* Administration on the move // Networks and communication systems. – 2007. – No. 14. – P. 43-52. – EDN ILJELV.

4. *Khomenko A.D.* Coordination of expert assessments with fuzzy inference in an intrusion detection system // Problems of information security. Computer systems. – 2009. – No. 4. – P. 42-50. – EDN LDGKYP.

5. *Ternovoy O.S.* Early detection of DDoS attacks based on statistical analysis // Prospects for the development of information technology. – 2011. – No. 6. – P. 212-215. – EDN RPDHNT.

6. *Borisov V.I., Shaburov A.S.* On the application of signature methods of information analysis in SIEM systems // Bulletin of the Ural Federal District. Security in the information sphere. - 2015. - No. 3 (17). - P. 23-27. - EDN VIYWEZ.

7. *Tokarev S.A.* Study of artificial intelligence algorithms for detecting network attacks // International Journal of Professional Science. - 2023. - No. 6. - P. 177-182. - EDN TKYRXE.

8. *Orlov G.A., Krasov A.V., Gelfand A.M.* Application of Big Data in the analysis of big data in computer networks // Science-intensive technologies in space research of the Earth. - 2020. - Vol. 12, No. 4. - P. 76-84. – DOI 10.36724/2409-5419-2020-12-4-76-84. – EDN RQQTOQ.

9. *Krasov AV, Gelfand AM, Korzhik VI* Building a trusted computing environment [et al.]. – SPb: Individual entrepreneur Petriv Roman Bogdanovich, 2019. – 108 p. – ISBN 978-5-6043143-2-6. – EDN RECXBI.

10. *Dushin S.E., Krasov A.V., Kuzmin N.N., Yakovlev V.B.* Synthesis of structurally complex nonlinear control systems: Systems with polynomial nonlinearities. – SPb: St. Petersburg Electrotechnical University "LETI" named after V.I. Ulyanova (Lenina), 2004. – 371 p.

11. *Branitsky A.A.* Combined approach to detecting network attacks based on signature analysis and computational intelligence methods // Regional informatics "RI-2016": Conference materials, St. Petersburg, October 26–28, 2016. – St. Petersburg: Politechnika-print, 2016. – P. 150. – EDN OTYTAX.

Статья поступила в редакцию 17 февраля 2024 г.
Принята к публикации 14 июня 2024 г.

Ссылка для цитирования: Макарова А.К., Гельфанд А.М., Поляничева А.В. Ретроспективный анализ методов обнаружения DoS атак в VoIP-системах // Национальная безопасность и стратегическое планирование. 2024. № 2(46). С. 25-41. DOI: https://doi.org/10.37468/2307-1400-2024-3-25-41

For citation: Makarova A.K., Gelfand A.M., Polyanicheva A.V. Retrospective analysis of methods for detecting DoS attacks in VoIP systems // National security and strategic planning. 2024. № 2(46). pp. 25-41. DOI: https://doi.org/10.37468/2307-1400-2024-2-25-41

Сведения об авторах:

МАКАРОВА АЛЕКСАНДРА КОНСТАНТИНОВНА – *магистрант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича (193232, Россия, Санкт-Петербург, пр. Большевиков, д. 22/1), Санкт-Петербург, Россия*
ORCID: https://orcid.org/0000-0001-7745-3364
SPIN-код: 5179-9199
e-mail: alex-ecureuil@mail.ru

ГЕЛЬФАНД АРТЕМ МАКСИМОВИЧ – *старший преподаватель кафедры защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича(193232, Россия, Санкт-Петербург, пр. Большевиков, д. 22/1), Санкт-Петербург, Россия*
SPIN-код: 6480-8953
e-mail: amgelfand@mail.ru

ПОЛЯНИЧЕВА АННА ВАЛЕРЬЕВНА – *старший преподаватель кафедры защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича(193232, Россия, Санкт-Петербург, пр. Большевиков, д. 22/1), Санкт-Петербург, Россия*
ORCID: https://orcid.org/0000-0003-1283-9180
SPIN-код: 5939-4865
e-mail: polyanicheva.av@sut.ru

Information about the authors:

MAKAROVA ALEKSANDRA K. – *Master's student of The Bonch-Bruevich Saint-Petersburg state university of telecommunications (193232, Russia, St. Petersburg, Bolshevikov Ave., 22/1), Saint-Petersburg, Russia*
ORCID: https://orcid.org/0000-0001-7745-3364
SPIN: 5179-9199
e-mail: alex-ecureuil@mail.ru

GELFAND ARTEM M. – *Senior Lecturer, Department of Secure Communication Networks of The Bonch-Bruevich Saint-Petersburg state university of telecommunications (193232, Russia, St. Petersburg, Bolshevikov Ave., 22/1), Saint-Petersburg, Russia*
SPIN: 6480-8953
e-mail: amgelfand@mail.ru

POLYANICHEVA ANNA V. – *Senior Lecturer, Department of Secure Communication Networks of The Bonch-Bruevich Saint-Petersburg state university of telecommunications (193232, Russia, St. Petersburg, Bolshevikov Ave., 22/1), Saint-Petersburg, Russia*
ORCID: https://orcid.org/0000-0003-1283-9180
SPIN: 5939-4865
e-mail: polyanicheva.av@sut.ru